CARLO GAVAZZI
Automation Components

CARLO GAVAZZI

Security Notes for Relevant Connectable Products

Information on how to report security issues

This information is relevant to the product UWP40RSEXXX, including:

a) The hardware of the product
b) The embedded firmware/software
c) The PC software known as **UWP 4.0 IDE**, freely available by the Carlo Gavazzi website, and necessary to set-up the **UWP40RSEXXX** solution

The following **email address** is the available channel to users to report any manufacturer cybersecurity issue: cybersecurity.cgc@gavazziacbu.it

The user will receive a follow up email reporting the taking over of his/her request within 2 working days since the initial notification.

The user will receive a follow-up about the status updates of the reported cybersecurity issue at each status change:

1) Taking over (**within 2 working days** since initial notification)
2) Confirmation/Rejection of the reported Cybersecurity flaw (after the initial assessment, depending on the impact of the cybersecurity threat)
3) Beginning of the relevant tracking process with the competent CERT if the cybersecurity flaw has been confirmed (**within 5 working days** since point -2- if the flaw is confirmed)
4) Mitigation process agreed with CERT (after agreement with CERT, depending on the impact of the cybersecurity issue)

Information on minimum security updates period

This information is relevant to the product UWP40RSEXXX, including:

a) The hardware of the product
b) The embedded firmware/software
c) The PC software known as **UWP 4.0 IDE**, freely available by the Carlo Gavazzi website, and necessary to set-up the **UWP40RSEXXX** solution

The minimum length of time for which security updates will be provided is until **December 31st, 2033.**